Security Quickie 5

This week's topic: Safe Web Browsing

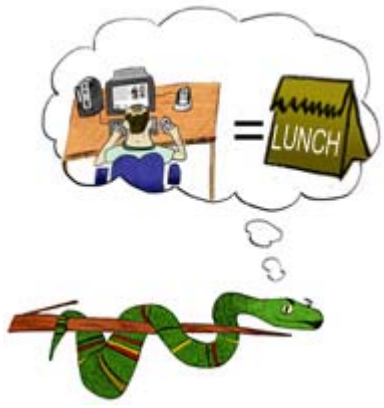
The Internet is rather like a jungle: vast, mysterious, full of useful resources and amazing sights, and it can be a boon for business or personal enjoyment. However, it has its pitfalls, snakes, nasty creatures that want to eat you, and dangerous places that you really want to avoid. Much like traveling in the jungle, one needs to take certain precautions when visiting the Internet.

Make sure your jeep is running well and your travel gear is in good order. That is, make sure your operating system and your web browser have current patches and fixes. If they don't, you may accidentally upload Trojan horse programs, worms, or allow personal information like credit card account numbers to be gathered by nefarious creatures that stalk the Internet.

Keep your eyes open and watch for potential danger. A firewall can help prevent unauthorized access to your computer and inform you of suspect Internet traffic. Most state agencies have firewall protection, but for web browsing from home, a personal firewall is recommended.

Wear protective clothing and stay inoculated. Use a virus scanner and make sure it's updated. Up to date virus protection will help tremendously in keeping nasty viruses and worms out of your system. (Especially if you access e-mail via the Internet/Intranet.)

Stay on the path. For business purposes, go to the jungle to get what you need, then go home. If your department allows web browsing and you are sight-seeing and doing some exploring during a break, be prudent in where you walk. Do not go to known hacker sites, and do not visit sites that your co-workers may find offensive. There are even some sites on the Internet that can attack your system simply by your visiting them - no downloads required. Just like with quicksand, when you realize you're in it, it is usually too late.



Leave the wildlife alone. Do not download anything unless you have the authorization to do so. The Law of the Jungle states: "shareware and freeware from any source shall be installed only with management approval" (ITD Operating Security Policy). Even if you are authorized to download from the Internet, it is best not to unless absolutely necessary. If you do have authorization and do download an item, scan it for viruses before opening or running it. Documents, executables, screen savers, videos, patriotic power point slideshows, or anything else - scan it.

Anyone can become prey. Please be aware that there are hackers out there that don't care who you are or what you are doing, you are simply a target to them. Like a very hungry carnivore in the jungle, they will eat you if they get the chance. Be mindful that some people are even using the Sept. 11 tragedies and associated issues to lure you to their sites in order to compromise your systems or to get credit card numbers to steal your money.

Remember that many bad things from the Internet jungle are contagious. The 1i0n worm, reputed Chinese hackers, and Russian credit card thieves are all examples of real threats. (Lions and Tigers and Bears, oh my!) If you get infected with a worm or virus, or a bad critter compromises your system, it could dramatically - and badly - affect your agency's network as well. In protecting your own system you are also protecting the state's network.